Department of Homeland Security

Privacy Office

Fourth Quarter Fiscal Year 2013 Report to Congress

December 2013

Homeland Security

Foreword

December 13, 2013

I am pleased to present the Department of Homeland Security (DHS or Department) Privacy Office's *Fourth Quarter Fiscal Year 2013 Report to Congress* for the period June 1 – August 31, 2013.[1]

Section 803 of the *Implementing Recommendations of the 9/11 Commission Act of 2007*[2] requires the DHS Privacy Office to report quarterly on the following activities:

- Number and types of privacy reviews of Department actions undertaken;
- Type of advice provided and the response given to such advice; and
- Number and nature of privacy complaints received by DHS for alleged violations, along with a summary of the disposition of such complaints.

In addition, we include information on privacy training and awareness activities conducted by the Department to help prevent privacy incidents.

The DHS Chief Privacy Officer is the first statutorily-mandated Chief Privacy Officer in the Federal Government. Section 222 of the *Homeland Security Act of 2002* (Homeland Security Act),[3] sets forth the responsibilities of the DHS Privacy Office. The mission of the DHS Privacy Office is to protect all individuals by embedding and enforcing privacy protections and transparency in all DHS activities. Within DHS, the Chief Privacy Officer implements Section 222 of the Homeland Security Act, the *Privacy Act of 1974*,[4] the *Freedom of Information Act*,[5] and the *E-Government Act of 2002*,[6] along with numerous other laws, executive orders, court decisions, and DHS policies that impact the collection, use, and disclosure of personally identifiable information by DHS.

Pursuant to Congressional notification requirements, the DHS Privacy Office provides this report to the following Members of Congress:

[1] The reporting period for this report corresponds with the period established for reporting under *The Federal Information Security Management Act of 2002* (FISMA, 44 U.S.C. § 3541) rather than the October through September fiscal year.
[2] 42 U.S.C. § 2000ee-1(f).
[3] 6 U.S.C. § 142.
[4] 5 U.S.C. § 552a.
[5] 5 U.S.C. § 552.
[6] 44 U.S.C. § 101 note.

The Honorable Thomas R. Carper
Chairman, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Tom Coburn, M.D.
Ranking Member, U.S. Senate Committee on Homeland Security and Governmental Affairs

The Honorable Patrick J. Leahy
Chairman, U.S. Senate Committee on the Judiciary

The Honorable Charles Grassley
Ranking Member, U.S. Senate Committee on the Judiciary

The Honorable Dianne Feinstein
Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Saxby Chambliss
Vice Chairman, U.S. Senate Select Committee on Intelligence

The Honorable Michael McCaul
Chairman, U.S. House of Representatives Committee on Homeland Security

The Honorable Bennie G. Thompson
Ranking Member, U.S. House of Representatives Committee on Homeland Security

The Honorable Darrell Issa
Chairman, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Elijah Cummings
Ranking Member, U.S. House of Representatives Committee on Oversight and Government Reform

The Honorable Bob Goodlatte
Chairman, U.S. House of Representatives Committee on the Judiciary

The Honorable John Conyers, Jr.
Ranking Member, U.S. House of Representatives Committee on the Judiciary

The Honorable Mike Rogers
Chairman, U.S. House of Representatives Permanent Select Committee on Intelligence

The Honorable C. A. Dutch Ruppersberger
Ranking Member, U.S. House of Representatives Permanent Select Committee on Intelligence

Please direct any inquiries about this report to the DHS Privacy Office at 202-343-1717 or privacy@dhs.gov. More information about the DHS Privacy Office, along with copies of prior reports, is available on the Web at: www.dhs.gov/privacy.

Sincerely,

Karen Neuman
Chief Privacy Officer
U.S. Department of Homeland Security

DHS PRIVACY OFFICE
FOURTH QUARTER FISCAL YEAR 2013
SECTION 803 REPORT TO CONGRESS

Table of Contents

II. LEGISLATIVE LANGUAGE

Section 803 of the *9/11 Commission Act of 2007*,[7] sets forth the following requirements:

"(f) Periodic Reports-

(1) In General –

The privacy officers and civil liberties officers of each department, agency, or element referred to or described in subsection (a) or (b) shall periodically, but not less than quarterly, submit a report on the activities of such officers—

(A)(i) to the appropriate committees of Congress, including the Committee on the Judiciary of the Senate, the Committee on the Judiciary of the House of Representatives, the Committee on Homeland Security and Governmental Affairs of the Senate, the Committee on Oversight and Government Reform of the House of Representatives, the Select Committee on Intelligence of the Senate, and the Permanent Select Committee on Intelligence of the House of Representatives;

(ii) to the head of such department, agency, or element; and

(iii) to the Privacy and Civil Liberties Oversight Board; and

(B) which shall be in unclassified form to the greatest extent possible, with a classified annex where necessary.

(2) Contents –

Each report submitted under paragraph (1) shall include information on the discharge of each of the functions of the officer concerned, including—

(A) information on the number and types of reviews undertaken;

(B) the type of advice provided and the response given to such advice;

(C) the number and nature of the complaints received by the department, agency, or element concerned for alleged violations; and

(D) a summary of the disposition of such complaints, the reviews and inquiries conducted, and the impact of the activities of such officer."

[7] 42 U.S.C. § 2000ee-1.

III. PRIVACY REVIEWS

The Department of Homeland Security (DHS or Department) Privacy Office (Office) reviews programs and information technology (IT) systems that may have a privacy impact.

For purposes of this report, reviews include the following DHS Privacy Office activities:

1. Privacy Threshold Analyses, the DHS foundational mechanism for reviewing IT systems, programs, and other activities for privacy protection issues to determine whether a more comprehensive analysis is necessary through the Privacy Impact Assessment process;

2. Privacy Impact Assessments, as required under the *E-Government Act of 2002*, the *Homeland Security Act of 2002*,[8] and DHS policy;

3. System of Records Notices, as required under the *Privacy Act of 1974*[9] (Privacy Act), and any associated Final Rules for Privacy Act exemptions;[10]

4. Privacy Act Statements, as required under the Privacy Act[11] to provide notice to individuals at the point of collection;

5. Computer Matching Agreements, as required under the Privacy Act;[12]

6. Data Mining Reports, as required by Section 804 of the *9/11 Commission Act of 2007*; [13]

7. Privacy Compliance Reviews, per the authority granted to the DHS Chief Privacy Officer by the *Homeland Security Act of 2002*;[14]

8. Privacy reviews of IT and program budget requests, including Office of Management and Budget (OMB) Exhibit 300s and Enterprise Architecture Alignment Requests through the DHS Enterprise Architecture Board; and

9. Other privacy reviews, such as implementation reviews for information sharing agreements.

[8] 6 U.S.C. § 142.
[9] 5 U.S.C. § 552a(e)(4).
[10] 5 U.S.C. § 552a(j), (k).
[11] 5 U.S.C. § 552a(e)(3).
[12] 5 U.S.C. § 552a(o)-(u).
[13] 42 U.S.C. § 2000ee-3.
[14] 6 U.S.C. § 142.

Table I: Reviews Completed Fourth Quarter Fiscal Year 2013	
Type of Review	**Number of Reviews**
Privacy Threshold Analyses	167
Privacy Impact Assessments	28
System of Records Notices and Associated Privacy Act Exemptions	2
Privacy Act (e)(3) Statements	1
Computer Matching Agreements	3
Data Mining Reports	0
Privacy Compliance Reviews	2
Privacy Reviews of IT and Program Budget Requests[15]	110
Other Privacy Reviews	0
Total Reviews	***313***

[15] The number increased this quarter because the Chief Information Office prepares a privacy score as part of its Office of Management and Budget-300 reporting, which is only completed once a year.

A. Privacy Impact Assessments

The Privacy Impact Assessment (PIA) process is one of the Department's key mechanisms to ensure that DHS programs and technologies sustain, and do not erode, privacy protections. As of August 31, 2013, 89 percent of the Department's *Federal Information Security Management Act* (FISMA) systems requiring a PIA had one in effect.

In addition to completing PIAs for new systems and systems not currently subject to a PIA, the Department conducts a triennial review of existing PIAs to assess and confirm that the systems still operate within the originally published parameters. After the Department completes a triennial review, it updates any previously published PIAs to inform the public that it has completed a review of the affected systems.

During the reporting period, the Office published 28 new, updated, or renewed PIAs, and four are summarized below. A hyperlink to the full text of each PIA listed here is included below. All published DHS PIAs are available on the DHS Privacy Office website, www.dhs.gov/privacy. Please consult our website for the full text of the PIAs summarized below.

DHS/CBP/PIA-001(f) - Advanced Passenger Information System Update National Counterterrorism Center (NCTC) (June 5, 2013); DHS/CBP/PIA-007(c) - Electronic System for Travel Authorization Update (June 5, 2013); and DHS/USCIS/PIA-027(b) - Refugees, Asylum, and Parole System and the Asylum Pre-Screening System Update (June 5, 2013)

Background: DHS shares bulk information with the National Counterterrorism Center (NCTC) from key DHS data sets, including the Advanced Passenger Information System (APIS), the Electronic System of Travel Authorization (ESTA), and the Refugees, Asylum, and Parole System (RAPS), in order to identify terrorism information within DHS data, and to support the NCTC's counterterrorism activities. In March 2012, the Attorney General of the United States approved the *Guidelines for Access, Retention, Use and Dissemination by the National Counterterrorism Center and other Agencies of Information in Data Sets Containing Non-Terrorism Information* (AG Guidelines). The AG Guidelines expand the period of time the NCTC is allowed to temporarily retain U.S. Person information to determine whether it constitutes terrorism information. In light of these new guidelines, the NCTC requested that DHS re-evaluate all of its information sharing and access agreements with the NCTC, including the agreements for APIS, ESTA, and RAPS.

Purpose: These PIAs address the NCTC's expanded temporary retention of U.S Person information in APIS (from 180 days to one year), as well as the NCTC's expanded temporary retention of RAPS information (from 180 days to three years). Although the NCTC's temporary retention period of two years for ESTA did not change, DHS completed a PIA to inform the public of the updated information sharing and access agreement for ESTA. Finally, consistent with the Fair Information Practice Principles (FIPPs), these PIAs provide additional transparency regarding DHS's sharing of bulk information with the NCTC.

***DHS/NPPD/PIA-002* Updates to the Automated Biometric Identification System - IDENT (December 7, 2012 with appendices revised June 25, 2013)**

Background: The Automated Biometric Identification System (IDENT) is the central DHS-wide system for storage and processing of biometric and associated biographic information for national security, law enforcement, immigration and border management, intelligence, background investigations for national security positions and certain positions of public trust, and associated testing, training, management reporting, planning and analysis, or other administrative uses.

DHS updated the appendix to the PIA twice to describe sharing between U.S. Department of Defense (DOD) and IDENT, and a signing of a new Preventing and Combating Serious Crime Agreement (PCSC) with the Republic of China (Taiwan). Current biometric data sharing between DOD and IDENT is performed manually; now biometrics will be transmitted through a secure File Transfer Protocol site. The two databases will now be able to search for known or suspected terrorists and national security threats as known to each other.. Additionally, the United States Government recently signed a PCSC with the Republic of China (Taiwan) to enhance and expedite cooperation in preventing and combating serious crime.

Purpose: This appendix update to the IDENT PIA provides transparency and a privacy impact analysis of how DHS shares data and biometrics with DOD and the Republic of China (Taiwan). It also provides an important view into how DHS fulfills its mission to identify threats to the homeland.

B. System of Records Notices

As of August 31, 2013, 98 percent of the Department's FISMA systems that require a System of Records Notice (SORN) had an applicable SORN. SORNs receive biennial reviews to ensure that they conform to and comply with the standards outlined in the Privacy Act. If no update is required, the original SORN remains in effect.

During the reporting period the Office published two SORNs which are summarized below. A hyperlink to the *Federal Register Notice* is included for each document listed here. All DHS SORNs, Notices of Proposed Rulemaking, and Final Rules for Privacy Act Exemptions are available on the DHS Privacy Office website, www.dhs.gov/privacy. Please consult our website for the full text of the SORNs summarized below.

DHS/FEMA-006 – Citizen Corps Program System of Records

In accordance with the Privacy Act of 1974, DHS updated and reissued a current DHS system of records notice titled, "Department of Homeland Security/Federal Emergency Management Agency (FEMA)--006 Citizen Corps Database" and retitled it "Department of Homeland Security/Federal Emergency Management Agency--006 Citizen Corps Program System of Records." This system of records allows FEMA to collect and maintain records on individuals who contact the agency about their interest in specific voluntary programs; members of the Citizen Corps Program who have been assigned disaster duties; and points of contact for Citizen Corps Councils, Community Emergency Response Teams, and Citizen Corps partners. As a result of a biennial review of this system, the SORN has been updated within the following sections: (1) system name; (2) categories of individuals; (3) categories of records; (4) authorities; (5) purpose; (6) routine uses of information; (7) system manager and address; (8) notification procedures; and (9) records source categories. Additionally, the notice includes non-substantive changes to simplify the formatting and text of the previously published SORN.

DHS/ALL -035 – Common Entity Index Prototype System of Records

This system of records allows the Department of Homeland Security to correlate identity data from select Component-level systems and organizes key identifiers that the Department of Homeland Security has collected about that individual. This correlation and consolidation of identity data will facilitate DHS's ability to carry out its vetting missions with appropriate privacy safeguards and access controls. DHS is building a prototype with an initial set of data for testing and evaluation purposes. If the system passes the testing and evaluation stage and DHS moves to an operational system, either this system will be updated or a new system of records notice will be published.

C. Privacy Compliance Reviews

The DHS Privacy Office uses Privacy Compliance Reviews (PCR) to ensure DHS programs and technologies implement and maintain appropriate privacy protections for PII. Consistent with the Office's unique position as both an advisor and oversight body for the Department's privacy-sensitive programs and systems, the PCR is a collaborative effort that helps improve a program's ability to comply with existing privacy compliance documentation, including PIAs, SORNs, and formal agreements such as Memoranda of Understanding and Memoranda of Agreement.

During the reporting period, the Office conducted two PCRs: one on the DHS Office of Operations Coordination and Planning, National Operations Center's Counterterrorism Operations Desk Database; and one on the Department's implementation of the 2011 U.S.-EU Passenger Name Record (PNR) Agreement.

PCRs may result in public reports or internal recommendations, depending upon the sensitivity of the program under review. Public PCR reports, including the report on the 2011 U.S.-EU PNR Agreement, are available on the DHS Privacy Office website, www.dhs.gov/privacy, under "Investigations and Compliance Reviews."

IV. ADVICE AND RESPONSES

A. Privacy Training and Awareness

During the reporting period, DHS conducted the following privacy training:

Mandatory Training

87,237 DHS personnel completed the mandatory computer-assisted privacy awareness training course, *Privacy at DHS: Protecting Personal Information*. This course is required for all personnel when they join the Department, and annually thereafter. The Executive Office of the President (EOP) requested permission to customize our mandatory online privacy training course to train all of the approximately 3,000 EOP employees on best practices for safeguarding PII.

New Employee Training

3,378 DHS personnel attended instructor-led privacy training courses, primarily privacy training for new employees:

- The DHS Privacy Office provides privacy training as part of the Department's bi-weekly orientation session for all new headquarters employees.
    - Many of the Component Privacy Officers[16] also offer privacy training for new employees when they onboard.
- The DHS Privacy Office provides monthly privacy training as part of the two-day *DHS 101* course, which is required for all new and existing headquarters staff.

Miscellaneous Training

- **Freedom of Information Act (FOIA) training**: The Office hosts an ongoing series of topical trainings on evolving FOIA issues. On June 25, 2013, the Office provided a FOIA overview to 21 staff in the DHS Operations Security Working Group.
- **Privacy Compliance Workshop**: In June 2013, 180 personnel from 45 federal agencies attended the DHS Privacy Office Privacy Compliance Workshop. This one-day workshop provided in-depth training on DHS privacy compliance best practices. The Office hosted the workshop in DHS facilities.
- **"DHS 201" International Attaché Training:** The Department's "DHS 201" training module is a week-long course designed to prepare DHS employees who serve as DHS attachés at U.S. embassies worldwide by providing them with basic information on each Component's international activities. The DHS Privacy Office provides an international privacy policy module to raise awareness among new attachés of the potential impact of global privacy policies. The Office trained 150 participants in five training sessions during the reporting period.
- **DHS Security Specialist Certification Course**: The Office provides privacy training each month to participants of the week-long Security Specialist Training Certification Program. During the reporting period, 60 staff from all DHS Components were trained.

[16] 10 DHS offices and components have a Privacy Officer.

- **Reports Officer Certification Course**: The Office provides privacy training to reports officers who prepare intelligence reports as part of the DHS Intelligence Enterprise certification program. During this reporting period, the Office trained 16 reports officers on privacy policy.

B. DHS Privacy Office Awareness & Outreach

Meetings & Events

- Georgetown Law Federal Government Practitioners Conference – On June 26, the Acting Chief Privacy Officer moderated a panel on Government in the Cloud, and discussed the privacy considerations for cloud migration at the eDiscovery for Federal Government Practitioners Conference at the Georgetown University Law Center.

- 2013 Federal CIO Council Boot Camp – On June 26, the Senior Director of Privacy Oversight presented on Appendix J of the National Institutes of Standards and Technology (NIST) Special Publication 800-53, rev. 4, explaining how attendees can better understand the new privacy controls. She also discussed best practices for privacy protection and social media.

- Joint Review of the 2011 U.S. – European Union (EU) Passenger Name Record (PNR) Agreement On July 8 and 9, the Acting Chief Privacy Officer led a joint review of the 2011 U.S. – EU PNR Agreement. The DHS Privacy Office, in conjunction with staff from U.S. Customs Border and Protection, Office of International Affairs, Office of the General Counsel, the Transportation Security Administration, and U.S. Immigrations and Customs Enforcement represented the Department. The Departments of State and Justice also participated on the U.S. delegation. The EU delegation was led by the European Commission's Directorate of Home Affairs with support from the European Commission's Directorate of Justice, the German Data Protection Commissioner's Office, and the French Ministry of Interior. In preparation for the Joint Review, the DHS Privacy Office issued a report that found DHS to be mostly compliant with the 2011 Agreement, and offered seven recommendations to improve privacy protections in the Department's use of PNR. The European Commission is currently drafting a report in which it will share with DHS its findings for comment.

C. Component Privacy Office Awareness & Outreach

Federal Emergency Management Agency

- Continued to provide privacy training to all new headquarters staff during Enter-On-Duty orientations.

Federal Law Enforcement Training Centers

- Met with multiple Federal Law Enforcement Training Center components to explain privacy issues with a focus on the privacy compliance process.

National Protection and Programs Directorate

- Published two privacy tips in the Office of Biometric Identity Management internal newsletter: one on how to protect children from identity theft; and one on how to safeguard PII in the SharePoint collaboration environment.
- Partnered with DHS Privacy Office staff to present on Privacy Threshold Analyses at the DHS Privacy Compliance Workshop.
- Provided specialized privacy training to the Office of Security and Compliance staff, covering privacy considerations for the operational use of social media. The training was a prerequisite for granting employees access to social media tools for the purpose of handling administrative investigations.
- Presented a Privacy 101 briefing to employees at the Office of Cybersecurity and Communications.
- Trained the Contracting Officer Representatives for the Office of Cybersecurity and Communications, covering privacy considerations for acquisitions, as well as core provisions for incorporation into NPPD acquisition vehicles to protect privacy.
- Published the *Privacy Update*, NPPD's quarterly privacy awareness publication, to keep employees abreast of privacy news and emerging issues surrounding technology. In this issue, NPPD highlighted the July 2013 release of the CIO Council's paper, *Privacy Best Practices for Social Media*. An NPPD Privacy Analyst was a key member of the working group that drafted this paper.
- Received NPPD's Empowerment Award, formal recognition of the team's efforts to ensure that all NPPD employees are empowered to safeguard PII and make more informed decisions in areas in which there may be an impact on an individual's personal privacy.

Office of Intelligence and Analysis

- Continued to provide privacy training to all new headquarters staff during Enter-On-Duty orientations.

Science and Technology Directorate

- Conducted a presentation entitled, "Building Privacy into Unmanned Aircraft Systems Operations," at the Public Safety Guidance on Unmanned Aircraft Systems Operations Conference in Annapolis, Maryland on June 13, 2013.
- Participated as a group facilitator at the DHS Privacy Compliance Workshop in Washington, DC on June 19, 2013.
- Attended the 2013 Computers, Freedom & Privacy Conference in Washington, DC on June 25 and 26, 2013.

Transportation Security Administration

- Disseminated a broadcast email message to 2,400 Transportation Security Administration employees on how to secure Sensitive PII before emailing it.

United States Citizenship and Immigration Services

- Hosted the third Annual Privacy Awareness Day with privacy events at both United States Citizenship and Immigration Services (USCIS) Headquarters and regional offices that included a privacy open house with educational seminars and the first regional shared drive clean-up event. Guest speakers included the Science and Technology Directorate's Privacy Officer presenting "*Be Smart: Using Mobile Devices and Apps,"* and the DHS Senior Security Officer presenting "*Operations Security and Safe Social Networking*."
- Published the USCIS Office of Privacy third quarter newsletter, featuring privacy compliance across the Component.
- Published multiple privacy tips on the USCIS intranet to convey the appropriate use, access, sharing, and disposing of PII.
- Completed 18 site visits and risk assessments of various USCIS facilities to provide recommendations to leadership on privacy risks, and how to improve privacy protections and awareness in each region.
- Developed a new specialized training entitled "*Understanding Privacy Incidents*," which defines a privacy incident, explains how to report an incident, and describes how the USCIS Office of Privacy mitigates a privacy incident.
- Developed a privacy incident pocket card with information on how to report a privacy incident.
- Conducted a privacy briefing entitled "*Privacy Program Overview and Priorities*," to the Central Region's district directors and field office directors to provide an overview of the USCIS Office of Privacy's policies, procedures, and processes; the purpose and function of the Regional Privacy Program; and how the Central Regional privacy officers can assist Central Region leadership to ensure compliance with privacy regulations, policies, and procedures.
- Conducted training entitled "*Security Authorization Process"* to Information Security System Officers on the role of privacy in the security authorization process.

United States Coast Guard

- Trained over 1,000 personnel on privacy protection best practices in preparation for the large-scale move from multiple locations to the new Coast Guard headquarters in Washington, DC.

United States Immigration and Customs Enforcement

- Presented on SORNs and information sharing best practices at the DHS Privacy Compliance Workshop on June 19, 2013.
- Participated in a panel discussion at the DHS Law Enforcement Information Sharing Roundtable on August 20, 2013, addressing the legal and privacy considerations in information sharing.

United States Secret Service

- Hosted a Privacy Awareness Day on June 25, 2013 to distribute informational materials, and to generate discussion with employees about privacy best practices.
- Issued privacy awareness posters and flyers to raise privacy awareness, and to encourage employees to focus on the need to protect PII.
- Disseminated a privacy compliance brochure for dissemination at trainings and presentations.
- Conducted a presentation on safeguarding PII on July 25, 2013, to the USSS Human Capital Division.
- Enhanced the USSS intranet page to disseminate information to employees about privacy compliance, guidelines, and tools. USSS also developed a social media section on the intranet, and posted all relevant policies and directives governing the use of social media by Secret Service employees for operational and non-operational purposes.

V. PRIVACY COMPLAINTS AND DISPOSITIONS

For purposes of Section 803 reporting, complaints are written allegations of harm or violation of privacy compliance requirements filed with the DHS Privacy Office or DHS Components or programs. The categories of complaints reflected in the following table are aligned with the categories detailed in the Office of Management and Budget's Memorandum M-08-21, *FY 2008 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*. U.S. citizens, Legal Permanent Residents, visitors, and aliens submit complaints.[17]

Table II: Type and Disposition of Complaints Received in the Reporting Period

Type of Complaint	Number of complaints received during the reporting period	Disposition of Complaint		
		Closed, Responsive Action Taken[18]	In Progress (Current Period)	In Progress (Prior Periods)
Process & Procedure	8	5	3	1
Redress	0	1	0	0
Operational	910	829	181	9
Referred	13	13	0	0
Total	***931***	***848***	***184***	***10***

.

DHS separates complaints into four categories:

1. ***Process and Procedure****:* Issues concerning process and procedure, such as consent, or appropriate notice at the time of collection.
    a. *Example*: An individual submits a complaint that alleges a program violates privacy by collecting Social Security numbers without providing proper notice.
2. ***Redress***: Issues concerning appropriate access and/or correction of PII, and appropriate redress of such issues.
    a. *Example*: Misidentifications during a credentialing process or during traveler inspection at the border or screening at airports.[19]
3. ***Operational***: Issues related to general privacy concerns, and concerns not related to transparency or redress.
    a. *Example:* An employee's health information was disclosed to a non-supervisor.
4. ***Referred****:* The DHS Component or the DHS Privacy Office determined that the complaint would be more appropriately handled by another federal agency or entity, and referred the

[17] See *DHS Privacy Policy Guidance Memorandum 2007-01, Regarding Collection, Use, Retention, and Dissemination of Information on Non-U.S. Persons.*

[18] These totals include complaints opened and closed during this reporting period, and complaints opened in prior reporting periods but closed during this reporting period.

[19] This category excludes FOIA and Privacy Act requests for access, which are reported annually in the Annual FOIA Report, and Privacy Act Amendment requests, which are reported annually in the DHS Privacy Office Annual Report to Congress.

complaint to the appropriate organization. This category does not include internal referrals within DHS. The referral category both serves as a category of complaints and represents responsive action taken by the Department, unless a complaint must first be resolved with the external entity.

a. *Example*: An individual has a question about his or her driver's license or Social Security number, which the DHS Privacy Office refers to the proper agency.

DHS Components and the DHS Privacy Office report disposition of complaints in one of the two following categories:

1. *Closed, Responsive Action Taken*: The DHS Component or the DHS Privacy Office reviewed the complaint and took responsive action. For example, an individual may provide additional information to distinguish himself from another individual. In some cases, acknowledgement of the complaint serves as the responsive action taken. This category may include responsive action taken on a complaint received from a prior reporting period.

2. *In Progress*: The DHS Component or the DHS Privacy Office is reviewing the complaint to determine the appropriate action and/or response. This category identifies in-progress complaints from both the current and prior reporting periods.

The following are examples of complaints received during this reporting period, along with their disposition:

United States Customs and Border Protection

Complaint: A foreign visitor on a visa contacted the CBP INFO Center regarding difficulty retrieving the automated I-94 form from the CBP website upon arrival in the United States, and requested assistance to remediate the problem.

***Disposition*:** The CBP INFO Center investigated the complaint and reviewed the complainant's I-94 in the CBP system, noting that the passport number listed had expired. The CBP INFO Center guided the complainant through the CBP website and showed the individual where to view and print the form. The complainant corrected the passport number with the Deferred Inspections Site to ensure that this problem would not occur again.

Complaint: The CBP INFO Center was contacted by a complainant who is a member of Global Entry (GE), a CBP Trusted Traveler Program. The complainant used the GE card the first time upon arrival, but was referred to secondary screening without explanation. During the complainant's interview in secondary, the complainant was asked about a misdemeanor arrest that was previously disclosed on the GE application, which took place four decades earlier. The complainant questioned why the GE was approved, only to be questioned later in secondary screening about the arrest that had been fully vetted during the GE enrollment interview.

***Disposition*:** The CBP INFO Center contacted the GE Program to advise them that the complainant was being referred to secondary screening despite being approved for the GE Program. In response to the complaint, the GE Program made modifications to the complainant's records so the individual would no longer be referred to secondary, other than randomly, during the normal screening process.

United States Immigration and Customs Enforcement

Complaint: The ICE Privacy Office received a complaint from an ICE detainee alleging an ICE employee in a detention facility improperly disclosed information concerning the detainee's private matters and immigration proceedings to another detainee at the facility.

***Disposition*:** The ICE Privacy Office referred the complaint to ICE's Office of Professional Responsibility (OPR) for additional inquiry because the complaint appeared to indicate an allegation of misconduct. ICE OPR determined that the allegation was unsubstantiated due to a lack of supportive information, as the inquiry did not uncover any evidence of an improper disclosure of the detainee's private matters and immigration proceedings. Therefore, the complaint was closed.

VI. CONCLUSION

As required by the 9/11 Commission Act, this quarterly report summarizes the DHS Privacy Office's activities from June 1 – August 31, 2013. The DHS Privacy Office will continue to work with the Congress, colleagues in other federal departments and agencies, and the public to ensure that privacy is protected in our homeland security efforts.